UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/816,080	03/26/2001	A-jung Kim	030681-291	7143

21839 7590 09/22/2006

BUCHANAN, INGERSOLL & ROONEY PC
POST OFFICE BOX 1404
ALEXANDRIA, VA 22313-1404

EXAMINER	
DADA, BEEMNET W	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 09/22/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/816,080
Filing Date: March 26, 2001
Appellant(s): KIM, A-JUNG

Charles F. Wieland III
Registration No. 33,096
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed June 19, 2006.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

6,678,379	Mayers et al.	01-2004

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 102

1. Claims 1-6 are rejected under 35 U.S.C. 102(e) as being anticipated by Mayers et al US Patent 6,678,379 B1 (hereinafter Mayers).

2. As per claim 1, Mayers teaches a key agreement method for secure communication in a multiple access system, the key agreement method comprising the steps of:

(a) a first user encoding a signal from a source by a bit sequence and transmitting the signal [column 9, lines 8-16];

(b) a second user who is a legitimate counterpart of the first user decoding the transmitted signal and measuring the decoded signal [column 9, lines 15-20];

(c) the second user adopting only bits, on a bit-by-bit basis, having the measured value beyond the threshold value which is predetermined (i.e., keeping bits that constitute predetermined sets of bases and discarding other bits) [column 9, lines 21-36 and column 6, lines 39-62];

(d) the second user informing the first user that the bits adopted are the n-th bits in the transmitted bit sequence, not telling the values of the bits (i.e., without telling the measurement results) [column 9, lines 21-23 and 29-40]; and

(e) the first and second users taking the adopted bits as a key string, and discarding the remaining bits [column 9, lines 21-44].

3. As per claim 2, Mayers further teaches the method further comprising the steps of:

(f) selecting a subset of bits from the key string shared by the first and second users and checking errors, if the error rate obtained in (f) is below a tolerable level, considering the

transmission safe, accepting the key string and obtaining a refined key string with amplification such as error correction process; and discarding the key adopted in the step (e) if the error rate obtained in (f) exceeds the tolerable level, returning to the step (a) and performing (a) through (f) until getting the key string which satisfies the condition (g) [column 8, lines 65 – column 9, lines 20].

4. As per claim 3, Mayers further teaches the method wherein the signal transmitted in the step (a) is susceptible to noise [column 9, lines 2-6].

5. As per claim 4, Mayers further teaches the method wherein the second user uses a receiver affected by mutual modulated noise by another transmitter [column 8, lines 46-60].

6. As per claim 5 and 6, Mayers further teaches the method wherein the threshold value of the step (c) is determined by the second user considering at least a transmission rate, a transmission error rate, and a degree of security [column 6, lines 39-32 and column 9, lines 1-10].

(10) Response to Argument

With respect to claim 1, in page 7, lines 23-30 of the Appeal Brief, Appellant argued, that Mayers does not adopt only bits having a measured value beyond a threshold value. Appellant further argued that, "in Mayers, if a sufficient number of bits meet a parity test, it is concluded that there is no eavesdropping activity. The bits that have been tested are discarded, and a shared key is produced from the remaining random series of bits. In contrast, and as recited in claim 1, the second system adopts only those bits having a measured value beyond the threshold value, and informs the first system of the bit positions of the selected bits. The

adopted bits are then used as a key string for the first and second systems. Mayers discloses instead to discard the bits that are actually tested, and utilize the remaining random series of bits to form the shared key."

Examiner would point out that, Mayers teaches a quantum key distribution method, by transmission of photon signals in different states that corresponds to bits [column 6, lines 39-59]. Examiner would point out that, the term "measuring the decoded signal" is not defined by the specification. As understood by the examiner a signal can be measured in multiple variables, such as signal strength, signal frequency, signal to noise ratio..., etc. In this case Mayers teaches quantum measurement of a received photon signal to identify a received quantum state. Specifically, Mayers teaches transmitting photon signals from a first user [column 6, lines 45-46 and column 9, lines 15-16], and a second user receiving the transmitted photon signals and measuring the photons (i.e., the received photons are measured trying to identify the received quantum state based on different sets of prearranged bases, column 8, lines 47-64, column 6, lines 46-48 and column 9, lines 16-19). Here, it is determined which bits correspond to a predetermined four sets of bases, and these bits are kept and the other bits are discarded (i.e., **Mayers teaches adopting bits having a measured value which corresponds to a predetermined four sets of bases**, and any bits having a measured value which is outside of these bases are discarded (which implies, adopting bits having a measured value beyond a threshold value which is predetermined) column 8, lines 62-67 and column 21-28). Mayers teaches adopting only bits having a measured value which beyond a threshold value which is predetermined (i.e., keeping bits that correspond to cases where selected bases constitute one of the four set of bases, and if all results are within an error rate that is tolerable range, see column 8, lines 65-column 9, line 36).

Appellant in page 8, lines 3-7 of the Appeal Brief, argued that, in the present invention it is the second system that determines which bits to use for the key string. In contrast, Mayers discloses that the parity of the measurement results are collated on a bitwise basis between the sending and receiving parities. Thus, both the sending and receiving parties in Mayers are involved in the testing procedure.

Examiner would point out that, claim 1 is an open ended claim and does not specifically exclude the sending user in determining which bits to use for the key string. Mayes teaches the claim limitation which recites, "the second user informing the first use that the bits adopted are the n-th bits in the transmitted bit sequence, not telling the value of the bits" (i.e., without telling the measurement results, see column 6 lines 46-57 and column 9, lines 15-23).

With respect to claim 2, Appellant argued that Mayers fails to teach if the transmission is considered safe, the key string is accepted and refined.

Examiner would point out that, Mayers teaches checking whether a parity is correct and if the results are perfect or if the error rate is within a tolerable range, the transmission is considered safe, and the key string is accepted [see column 9, lines 1-6 and lines 29-41].

With respect to claim 4, Appellant argued that Mayers fails to teach mutual modulated noise by another transmitter.

Examiner would point out that, Mayers teaches transmitting signals through a classical public channel [see figure 1, 306], which inherently implies the second user uses a receiver affected by mutual modulated noise by another transmitter [see figure 1, units 301, 302, 306 and column 8, lines 53-55].

With respect to claims 5 and 6, Appellant argued that Mayers fails to teach the second user determining the threshold value of step c, considering at least three factors; transmission rate, transmission error rate and degree of security.

Examiner would point out that Mayers teaches measuring a threshold value which is predetermined (i.e., keeping bits that correspond to cases where selected bases constitute one of the four set of bases, and if all results are within an error rate that is tolerable range, see column 8, lines 65-column 9, line 36).

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Conferees:

Beemnet W Dada

Kim Vu KV

Kimbiz Zand KZ

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100